UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,599	10/09/2003	Steven T. Kirsch	ABC-008	1023

3897 7590 04/30/2008
SCHNECK & SCHNECK
P.O. BOX 2-E
SAN JOSE, CA 95109-0005

EXAMINER	
LAI, MICHAEL C	
ART UNIT	**PAPER NUMBER**
2157	

MAIL DATE	DELIVERY MODE
04/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/683,599	**Applicant(s)** KIRSCH, STEVEN T.
	Examiner MICHAEL C. LAI	**Art Unit** 2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2008*.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14 and 16-46* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-14,16,18-27,29-33,35-39,41 and 43-46* is/are rejected.
7)☒ Claim(s) *17,28,34,40 and 42* is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *9 oct 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)☐ All b)☐ Some * c)☐ None of:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is responsive to amendment filed on 3/28/2008.

Response to Amendment

The examiner has acknowledged the amended claims 1, 3, 5, 10-13, 16-17, 19, 21, 24-25, 30, 44, and the cancelled claim 15. The examiner failed to raise the double patenting issue in previous office actions. It is addressed in this action.

Response to Arguments

Applicant's arguments, see pages 23-24, filed 3/28/2008, with respect to 112 rejections have been fully considered and are persuasive. The 112 rejection of claims 1-46 has been withdrawn.

Applicant's arguments with respect to 102 rejection of claims 1-46 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-3, 6, 10-13 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 8-9 of U.S. Patent No. 7,206,814 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because (see the following table):

Instant Application 10/683,599	Patent No. 7,206,814
1. A method to categorize e-mail messages received in a network, the method comprising: a) receiving information about an e-mail message sent to a recipient within an e-mail network, the received information including at least one of the following: i) an actual sender of the e-mail message; ii) a final IP address used by the sender; iii) a final domain name used by the sender; and iv) an IP path used by the sender; b) storing the information; c) calculating statistics based on the stored information; d) using the calculated statistics to determine whether the received e-mail is unsolicited e-mail; and e) setting a predetermined threshold for accepting messages based on statistics associated with one of the following: i) an actual sender; ii) a final IP address; iii) a final domain name used; or iv) an IP path;	1. In a network, a method of processing e-mail messages comprising: a) receiving an e-mail message from an unknown sender; b) requesting information about the sender from at least one database that compiles global statistics about senders based on information about the sender received from recipients in the network, wherein compiling statistics includes determining a ratio reflecting whether the sender sends a majority of messages to recipients who have included the sender on a whitelist, wherein the statistics are used to determine a sender's reputation, wherein the sender is identified based on data in the message header including at least one of the following: i) an actual sender; ii) a final IP address used by the sender; iii) a final domain name used by the sender; or iv) an IP path used by the sender; and c) categorizing whether the e-mail message is good based on information received about the sender's reputation, wherein the e-mail message is allowed through a recipient's e-mail filter it the reputation as good and the e-mail message is not allowed through the e-mail filter if the reputation is either not good or not known.
2. The method of claim 1 wherein the actual sender is identified by a signature that includes at least two of the following fields from the message header; a) an e-mail address used by the sender; b) a display name used by the sender; c) a domain name used by the sender; d) the final IP address used by the sender;	2. The method of claim 1 wherein the actual sender is identified by a signature that includes at least two of the following fields from the message header; a) an e-mail address used by the sender; b) a display name used by the sender; c) a domain name used by the sender; d) a final IP address used by the sender; e) a final domain name used by the

e) the final domain name used by the sender; f) a client software name used by the actual sender; g) a user-agent; h) a timezone; i) source IP address; j) sendmail version used by a first receiver; and k) the IP path used to route the message.	sender; f) a user-agent; g) a timezone; h) a source IP address; i) a name of client software used by the sender; j) a sendmail version used by a first receiver; and k) an IP path used to route the message.
3. The method of claim 1 wherein the actual sender is identified by a signature including a range of IP addresses and at least one of the following fields from a message header: a) an e-mail address used by the sender; b) a display name used by the sender; c) a domain name used by the sender; d) the final IP address used by the sender; e) the final domain name used by the sender; f) a client software name used by the actual sender; g) user-agent; h) timezone; i) source IP address; j) sendmail version used by a first receiver; and k) the IP path used to route the message.	3. The method of claim 1 wherein the actual sender is identified by a signature including a range of IP addresses and at least one of the following fields from the message header: a) an e-mail address used by the sender; b) a display name used by the sender; c) a domain name used by the sender; d) the final IP address used by the sender; e) the final domain name used by the sender; f) the name of client software used by the actual sender; g) user-agent; h) timezone; i) source IP address; j) sendmail version used by a first receiver; and k) the IP path used to route the message.
6. The method of claim 1 wherein information stored about the actual sender includes at least one of the following: a) a total number of messages sent; b) a total number of messages sent over a first predetermined time period; c) a total number of messages sent to recipients in the network who have included the sender on a whitelist; d) a number of messages sent to recipients in the network who have included the actual sender on the whitelist	8. The method of claim 1 further comprising tracking at least one of the following pieces of information about messages from senders: a) a total number of messages sent; b) a total number of messages sent over a first predetermined time period; c) a total number of messages sent to recipients in the network who have included the sender on a whitelist; d) a number of messages sent to recipients in the network who have

over a second predetermined time period; e) a number of recipients who know the actual sender; f) a total number of times a recipient changed whitelist/blacklist status of the actual sender; g) a number of times any recipient changed the actual sender's whitelist/blacklist status over a third predetermined time period; h) a total number of messages sent to recipients in the network who don't know the actual sender; i) a number of messages sent to recipients in the network who don't know the actual sender over a fourth predetermined time period; j) a total number of unique recipients in the network who have received at least one message from the actual sender; k) a total number of messages sent to unique recipients in a network who have included the actual sender on a whitelist; and l) a total number of messages sent to unique recipients in the network who have not included the actual sender on the whitelist.	included the sender on the whitelist over a second predetermined time period; e) a number of recipients who have included the sender on the recipient's whitelist; f) a total number of times a recipient changed a sender's whitelist/blacklist status; g) a number of times a recipient changed a sender's whitelist/blacklist status over a third predetermined time period; h) a total number of messages sent to recipients in the network who have not included the sender on the whitelist; i) a number of messages sent to recipients in the network who have not included the sender on the whitelist over a fourth predetermined time period; j) a total number of unique recipients in the network who have received at least one message from the sender; k) a total number of messages sent to unique recipients in the network who have included the sender on the whitelist; and l) a total number of messages sent to unique recipients in the network who have not included the sender on the whitelist, wherein the sender is identified by one of the group consisting of the actual sender, the final IP address, the final domain name, or the IP path used to send the message..
10. The method of claim 1 wherein the step of calculating statistics includes at least one of the following: a) determining a ratio of a first number e-mail messages sent by an actual sender to recipients in the network who have included the sender on a whitelist in a predetermined time period divided by a second number of e-mail messages sent by the sender to users in the network in	9. The method of claim 1 wherein compiling statistics about senders includes at least one of the following: a) determining a ratio of a first number e-mail messages sent by a sender to recipients in the network who have included the sender on a whitelist in a predetermined time period divided by a second number of e-mail messages sent by the sender to users in the network in

the predetermined time period; b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from the sender in a predetermined time period; c) determining a ratio of a first number of times in a predetermined time interval a message from the actual sender was moved from a whitelist to a blacklist divided by a second number of times a message from the sender was moved from a whitelist to a blacklist; d) determining a ratio of a first number of times in a predetermined time interval a message from the actual sender was moved from a blacklist to a whitelist divided by a second number of times a message from the sender was moved from a blacklist to a whitelist; e) determining a ratio of a first number of unique users within the network who whitelisted the actual sender within a predetermined time period compared to a second number of unique users within the network who blacklisted the sender within the predetermined time period; f) determining a ratio reflecting whether the actual sender sends a majority of messages to recipients who have included the actual sender on the whitelist; g) determining a ratio reflecting a first number of wanted messages sent by the actual sender compared to a second number of unwanted or total messages sent by the actual sender; h) determining a difference between a first number of expected messages sent by the actual sender and a second number of unexpected ed messages sent by the actual sender; i) determining a difference between a first	the predetermined time period; b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from the sender in a predetermined time period; c) determining a ratio of a first number of times in a predetermined time interval a message from the sender was moved from a whitelist to a blacklist divided by a second number of times a message from the sender was moved from a whitelist to a blacklist; d) determining a ratio of a first number of times in a predetermined time interval a message from the sender was moved from a blacklist to a whitelist divided by a second number of times a message from the sender was moved from a blacklist to a whitelist; e) determining a ratio of a first number of unique users within the network who whitelisted the sender within a predetermined time period compared to a second number of unique users within the network who blacklisted the sender within the predetermined time period; f) determining a ratio reflecting a first number of wanted messages sent by the sender compared to a second number of unwanted or total messages sent by the sender; g) determining a difference between a first number of expected messages sent by the sender and a second number of unexpected messages sent by the sender; h) determining a difference between a first number of times a user whitelisted a message from the sender and a second number of times a user blacklisted a message from the sender; and i) determining a difference reflecting

number of times a user whitelisted a messages the actual sender and a second number of times a user blacklisted a message from the actual sender; j) determining a difference reflecting whether the actual sender sends a majority of messages to known recipients; k) converting any of the above ratios or differences to a score indicating the likelihood the message is unsolicited e-mail; and l) applying the score to the appropriate message in the spam folder. Claims 11-13 are similar to claim 10.	whether the sender sends a majority of messages to known recipients, wherein the sender is identified by one of the group consisting of the actual sender, the final IP address, the final domain name, or the IP path used to send the message.

Claim Objections

3. Claims 4, 35 and 38 are objected to under 37 CFR 1.75(c) as being in improper form because they depend on a future claim (44, 46 and 44 respectively). See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 10-13 recite the limitation "in the spam folder" in item "l)". There is insufficient antecedent basis for this limitation in the claims.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an

> application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-14, 16, 18-27, 29-33, 35-39, 41 and 43-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Goldman (US 20030233418 A1), hereinafter referred to as Goldman.

8. Regarding claim 1, Goldman discloses a method to categorize e-mail messages received in a network, the method comprising: a) receiving information about an e-mail message sent to a recipient within an e-mail network, the received information including an actual sender of the e-mail message (page 3, paragraph 0038: In general, incoming electronic message 38 includes a recipient's address 55 and may or may not include a sender's address 57.); b) storing the information (page 3, paragraph 0038: the incoming electronic message is stored at a mailbox 20 of the data storage device 19.); c) calculating statistics based on the stored information (page 1, paragraph 0008: The present invention also relates to a request/response technique for categorizing a sender's address as authorized, unauthorized, or unconfirmed, which categorizations are **stored** in an associated data structure. In addition, the present invention provides a number of complementary techniques for facilitating the **process** of populating the data structures that identify sender's addresses associated with authorized and unauthorized senders.); d) using the calculated statistics to determine whether the received e-mail is unsolicited e-mail (page 1, paragraph 0010: The filter module filters out unsolicited electronic messages according to various protocol set forth herein.); and e) setting a predetermined threshold for accepting messages based on statistics associated with an

actual sender (page 1, paragraph 0010: The unconfirmed category management module recategorizes sender's addresses that have been categorized as unconfirmed for **a predetermined period of time**. The outgoing mail categorization module allows a user to cause recipient's addresses in outgoing electronic messages to be automatically categorized as authorized.).

9. Regarding claim 2, Goldman further discloses the actual sender is identified by a signature that includes an e-mail address used by the sender and a domain name by the sender (page 4, paragraph 0045).

10. Regarding claim 3, Goldman further discloses the actual sender is identified by a signature including a rage of IP addresses and an e-mail address used by the sender (page 4, paragraph 0045).

11. Regarding claim 4, Goldman further discloses storing information about received messages in the at least one database, the information including information identifying the actual sender and whether the actual sender is included on a recipient's whitelist (page 1, paragraph 0008, “The present invention also relates to a request/response technique for categorizing a sender's address as authorized, unauthorized, or unconfirmed, which categorizations are stored in an associated data structure”);

12. Regarding claim 5, Goldman further discloses storing the recipient statistics such as an actual sender (page 3, paragraph 0039, lines 5-10).

13. Regarding claim 6, Goldman further discloses wherein information stored about an actual sender includes a total number of messages sent (page 4, paragraph 0045, lines 1-2).

14. Regarding claim 7, Goldman further discloses wherein information stored about messages sent from a final IP address includes a total number of messages sent (page 3, paragraph 0033: the operation of electronic mailing systems over the Internet).

15. Regarding claim 8, Goldman further discloses wherein information stored about messages sent from a final domain name includes a total number of messages sent (page 4, paragraph 0045, lines 7-14).

16. Regarding claim 9, Goldman further discloses wherein information stored about messages sent using an IP path includes a total number of messages sent (page 3, paragraph 0033: the operation of electronic mailing systems over the Internet).

17. Regarding claims 10-13, Goldman further discloses wherein the step of calculating statistics includes applying the score to the appropriate message in the spam folder (page 2, paragraph 0032: "unsolicited"; page 5, paragraph 0053).

18. Regarding claim 14, Goldman further discloses revising statistics when a recipient changes a whitelist/blacklist status of an actual sender (FIG. 4, AUTHORIZED, UNAUTHORIZED; page 4, paragraph 0045: sender's addresses located in data structure 18 may be added, deleted, modified, or transferred from one category to another.).

19. Regarding claim 16, Goldman further discloses accepting messages when information about the message exceeds the predetermined threshold (page 8, paragraph 0082: If the time interval does exceed a predetermined time interval, the system advances to step 48.).

20. Regarding claim 18, Goldman further discloses monitoring a recipient's spam folder at predetermined intervals to determine whether messages should be released (page 5, paragraph 0053: At step 68, if the sender's address is already categorized as unconfirmed, the electronic message is sent to a folder associated with the mail processor, such as an unconfirmed folder, to await confirmation that the sender's address is either authorized or unauthorized. If, however, the sender's address is also not yet unconfirmed, the electronic message is also sent to the unconfirmed folder and the process of confirming whether the sender's address is either authorized or unauthorized is initiated in step 47).

21. Regarding claim 19, Goldman further discloses automatically releasing the message from the spam folder when the reputation of an actual sender passes the predetermined threshold (page 5, paragraph 0053).

22. Regarding claim 20, Goldman further discloses reevaluating the spam folder immediately before it is displayed to the recipient such that information about messages in the spam folder is current when viewed by the recipient (page 5, paragraph 0053).

23. Regarding claim 21, Goldman further discloses when revising the statistics, more heavily weighting a manual reversal of the whitelist/blacklist status of an actual sender (page 7, paragraph 0074: manually authorized by recipient).

24. Regarding claim 22, Goldman further discloses wherein information about the final IP address is sent to the recipient when there is insufficient information about the actual sender (page 3, paragraph 0033: the operation of electronic mailing systems over the Internet).

25. Regarding claim 23, Goldman further discloses using the calculated statistics to compute a score indicating a likelihood that the received message is unsolicited e-mail (page 4, paragraph 0050: At step 56, if a sender's address is not associated with incoming message 38 or if the message is not properly addressed to the recipient, the incoming message 38 is assumed to be unsolicited).

26. Regarding claim 24, Goldman further discloses each user setting a predetermined personalized spam threshold, wherein an incoming message that exceeds the spam threshold is sent to a folder designated to hold spam messages (page 4, paragraph 0050: The techniques for filtering electronic messages are described herein primarily in combination with deleting electronic messages of unauthorized senders or placing them in a trash bin. However, the use of any other mechanism to segregate or differentiate electronic messages of authorized, unauthorized, and unconfirmed senders can be used. For instance, any desired set of folders or message boxes can be used, as well as sorting electronic messages based on the categorization of the sender, or the use of various colors, fonts, icons, or other visual mechanism to represent the categorization of the sender).

27. Regarding claim 25, Goldman further discloses each user setting a predetermined personalized delete threshold, wherein an incoming message that exceeds the delete threshold is deleted (page 7, paragraph 0071: The system or the recipient may decide how much time lapses between when an electronic message 38 is sent from the unconfirmed folder to the trash bin. Furthermore, the system or the

recipient may determine how much time lapses between when an electronic message 38 in the trash bin is to be automatically deleted.).

28. Regarding claim 26, Goldman further discloses maintaining a number of messages whose ranking is unknown; wherein the values are based on messages having the same information about the sender including an actual sender (page 4, paragraph 0044: The "unconfirmed" category 74 includes any sender's address that has not yet been categorized as authorized or unauthorized).

29. Regarding claim 27, Goldman further discloses wherein the values represent ratings of unique users within the network (page 5, paragraph 0050: However, the use of any other mechanism to segregate or differentiate electronic messages of authorized, unauthorized, and unconfirmed senders can be used. For instance, any desired set of folders or message boxes can be used, as well as sorting electronic messages based on the categorization of the sender, or the use of various colors, fonts, icons, or other visual mechanism to represent the categorization of the sender.).

30. Regarding claim 29, Goldman further discloses evaluating an unknown sender based on statistics of a known final IP address used by the sender (page 5, paragraph 0053: At step 68, if the sender's address is already categorized as unconfirmed, the electronic message is sent to a folder associated with the mail processor, such as an unconfirmed folder, to await confirmation that the sender's address is either authorized or unauthorized. If, however, the sender's address is also not yet unconfirmed, the electronic message is also sent to the unconfirmed folder and the process of confirming whether the sender's address is either authorized or unauthorized is initiated in step 47).

31. Regarding claim 30, Goldman further discloses evaluating an unknown sender using either a known final IP address or a known final domain name based on statistics about other new senders using either the known final IP address or the known final domain (paragraph 0045, paragraph 0053: At step 68, if the sender's address is already categorized as unconfirmed, the electronic message is sent to a folder associated with the mail processor, such as an unconfirmed folder, to await confirmation that the sender's address is either authorized or unauthorized. If, however, the sender's address is also not yet unconfirmed, the electronic message is also sent to the unconfirmed folder and the process of confirming whether the sender's address is either authorized or unauthorized is initiated in step 47).

32. Regarding claim 31, Goldman further discloses giving an unknown final IP address or final domain name an initial good rating (paragraph 0044: The "unconfirmed" category 74 includes any sender's address that has not yet been categorized as authorized or unauthorized. An "unconfirmed" electronic message may or may not be unsolicited; paragraph 0045.).

33. Regarding claim 32, Goldman further discloses giving an unknown final IP address or domain name an initial rating based on the length of time the network has been in operation (FIG. 10, step 97, paragraph 0085).

34. Regarding claim 33, Goldman further discloses using message ratings of earlier members of the network to overwrite the message ratings of later members of the network when the message ratings of the later members of the network are inconsistent with the message ratings of the earlier members of the network (paragraph 0075,

conflict resolution: Any combination of these embodiments may be provided or selected by the recipient depending on how stringent or relaxed the system or recipient desires the filtering of electronic messages to be.).

35. Regarding claim 35, Goldman further discloses wherein personal statistics are checked at the local database before global statistics at either the central database or the at least two centrally-maintained databases are checked (paragraph 0098, lines 7-10; FIG. 13, and paragraphs 0102 and 0103).

36. Regarding claim 36, Goldman further discloses rating a sender by: a) releasing a small number of a sender's messages to recipients; and b) monitoring a classification of the sender's messages received from the recipients (paragraph 0053).

37. Regarding claim 37, Goldman further discloses changing a first user's rating when a plurality of other users outvote the first user's rating (paragraph 0096).

38. Regarding claim 38, Goldman further discloses wherein one or more of the at least one database returns more than one value of ranking to the recipient (paragraph 0075).

39. Regarding claim 39, Goldman further discloses monitoring the inbox at predetermined intervals to determine whether messages should remain in the inbox (paragraphs 0081, 0082).

40. Regarding claim 41, Goldman further discloses categorizing a received message that cannot be rated locally when user activity is observed (paragraph 0085).

41. Regarding claim 43, Goldman further discloses sending recipients a notification when any sender's reputation changes (paragraphs 0081, 0082).

42. Regarding claim 44, Goldman further discloses the method of claim 1 further comprising: maintaining at least one database; and including in the at least one database: a central database (paragraph 0008).

43. Regarding claim 45, Goldman further discloses the method of claim 44 comprising storing the received information in the at least database (paragraph 0045).

44. Regarding claim 46, Goldman further discloses the method of claim 44 comprising maintaining the calculated statistics in the at least one database (paragraph 0056).

Allowable Subject Matter

45. Claims 17, 28, 34, 40, 42 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

46. Goldman doesn't disclose: setting a low threshold to differentiate wanted messages from unsolicited messages, wherein the low threshold is either: a) greater than one percent of a number of messages are accepted, wherein the messages are characterized by one of the following: i) an actual sender; ii) a final IP address; iii) a final domain name; or iv) an IP path; b) greater than one percent of a number of unique users accepting a message characterized by one of the following: i) an actual sender; ii) a final IP address; iii) a final domain name; or iv) an IP path (claim 17); at least four of the values (mentioned in claim 26) being returned to the recipient to allow the recipient to apply different weights to a message in order to categorize the message (claim 28); a final message score is determined by one of the following: a) an average of two scores

for a message; or b) a product of two scores for the message; wherein the scores for messages are based on statistics associated with a least two of the following: i) an actual sender of the message; ii) a final IP address used by the sender; iii) a final domain name used by the sender; or iv) an IP path used by the sender (claim 34); a first score for an unknown sender using a known final IP address or final domain name may be obtained by multiplying a second score for the final IP address or final domain name by a number less than one (claim 40); using a second formula to compute the score for the message when the message is reevaluated, wherein the second formula differs from a first formula used to compute the previous message score (claim 42).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Rothwell et al. (US 7,209,954 B1) discloses a method for intelligent spam detection by using statistical analysis.

Examiner's Note: Examiner has cited particular paragraphs and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael C. Lai whose telephone number is (571) 270-3236. The examiner can normally be reached on M-F 8:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael C. Lai
26APR2008

/Yves Dalencourt/
Primary Examiner, Art Unit 2157